LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Verkon Segmentaatio

Vuorela, Oskar

2015 Laurea Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Verkon Segmentaatio

Oskar Vuorela
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Kuukausi, 2015

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Tietojenkäsittelyn koulutusohjelma

Oskar Vuorela

Verkon segmentaatio

Vuosi 2015 Sivumäärä 20

Kevään 2014 tietomurrot aiheuttivat useille yrityksille vakavia vahinkoja. Tämän opinnäytetyön tavoite on ollut tutkia yritysverkon segmentaation hyötyjä yrityksen tietoturvan kannalta. Työssä tutkitaan segmentaatiota ja sen hyödyntämismahdollisuuksia Active Directoryn ja Oracle Databasen yhteydessä.

Työ toteutettiin pääkaupunkiseudulla sijaitsevalle PK-yritykselle. Yritys tarvitsi edellä mainittujen tietomurtojen takia analyysin segmentaation toteuttamisesta. Tämä raportti tuotettiin täyttämään edellä mainittu tarve.

Työn tietoperusta on koottu internet-lähteistä sekä kohdeyrityksen toimintaympäristöstä. Työ suunniteltiin ja toteutettiin kohdeyrityksessä.

Projektin kautta kohdeyritys sai tarvitsemansa parannuksen tietoturvaan VLAN-segmentaation kautta.

Asiasanat: VLAN, Active Directory, RADIUS, Oracle Database

Laurea University of Applied Sciences **Abstract**
Leppävaara
Programme

Oskar Vuorela

Network segmentation

Year 2015 Pages 20

The information security breaches of 2014 caused severe damage to many companies. The goal of this thesis has been to investigate the benefits of corporate network segmentation. Network segmentation and the possibilities of using it with Active Directory and Oracle Database are investigated in the thesis.

The report was produced for a small- to medium-sized company in capital city area. The company required an analysis of the deployment of network segmentation due to the aforementioned security breaches. This report was produced to fulfill the aforementioned need.

The knowledge base of the report is based on internet-sources and the operating environment of the company. The report was designed and its results deployed in the target company.

The target company acquired the improvement in information security it needed through the project.

Keywords: VLAN, Active Directory, RADIUS, Oracle Database

Sisällys

1 Johdanto

Tarve yrityksen verkon VLAN-segmentointiin syntyi alun perin tietoturvasyistä, tarkemmin kevään 2014 tietomurroista, sekä myös osalta edellisen verkon hitauden korjaamiseen. Työn tarkoituksena on tutkia pienen-keskisuuren yrityksen tietoverkon tietoturvan parantamista verkon segmentaation avulla. Omat oppimistavoitteet ovat tiedon ja kokemuksen lisääminen aiheesta. Hankeorganisaationa toimii pääkaupunkiseudulla toimiva PK-yritys. Hankeorganisaatio tarjoaa toimintaympäristön ja paikan työskennellä.

Tutkimusongelmana on pienen-keskisuuren yrityksen tietoverkon tietoturvan parantaminen verkon segmentaation avulla. Tutkimuskysymyksinä ovat ”Miten verkon segmentaatio parantaa tietoverkon tietoturvaa?”, ”Mikä on sopivin tapa pienelle-keskisuurelle yritykselle segmentoida tietoverkkonsa?”. Työn tavoitteena on hankeyrityksen tietoturvan parantuminen toimivan VLAN-segmentaation ja Active Directory- sekä Oracle Database-integraation kautta.

Työn pääasiallinen tarkoitus on tuottaa hyöty tietoturvan parantumisessa hankeyritykselle. Tästä huolimatta se on yleiskäyttöinen tutkimus segmentaatiosta ja ohje sen käyttöön.

Työn viitekehyksenä toimii internet- ja mahdollisesti kirjapohjainen materiaali aiheesta, ja työn keskeiset käsitteet ovat VLAN, RADIUS, Oracle Database ja Microsoft Active Directory. Ulkoisten lähteiden lisäksi työ käyttää hankeyrityksen toimintaympäristöä esimerkkinä ja pohjana verkon segmentaation suunnitteluun käytännössä.

Opinnäytetyössä on tietoperusta, jossa käydään läpi peruskäsitteet. Tämän jälkeen on kolmantena kappale, jossa selitään segmentaatio teoreettisesti. Neljäntenä on segmentaatiota ja Active Directory-suunnittelua käytännössä käsittelevä kappale, viidentenä langattomia lähiverkkoja käsittelevä kappale, ja kuudentena Oracle-tietokanta-integraatiota käsittelevä kappale. Seitsemäntenä on käyttäjäoikeuksia käsittelevä kappale ja viimeisenä yhteenveto.

2 Tietoperusta

Tutkielmassa käytettiin useita eri internet-tietolähteitä. Seuraava osio selittää peruskäsitteet.

Active Directory on Microsoftin kehittämä hakemistopalvelu, joka on suunniteltu prosessoimaan suuria määriä luku- ja etsintäoperaatioita ja huomattavasti pienempiä määriä muutoksia. (”So What Is Active Directory?”, Microsoft 2014)

Active Directory Domain Services on Windows 2000 Server-, Windows Server 2003- ja Microsoft Windows Server 2008-käyttöjärjestelmien päälle rakennettujen jaettujen verkkojen pohjajärjestelmä. Järjestelmä tarjoaa turvallista, hierarkkista datasäilytystä verkkoobjekteille kuten käyttäjille, tietokoneille, tulostimille ja palveluille. (”Active Directory Domain Services”, Microsoft 2014)

OU (Organizational Unit) on Active Directory container, johon voi sijoittaa mm. käyttäjiä, ryhmiä, tietokoneita. (”Organizational units”, Microsoft 2005)

Payment Card Industry Data Security Standard (PCI DSS) on maksukorttiyhtiöiden käyttämä tietoturvastandardi. Se kehitettiin parantamaan kortinhaltioiden tietoturvallisuutta ja helpottaa maailmanlaajuisesti vastaavien tietoturvakäytänteiden laajaa käyttöönottoa. (“PCI Data Security Standard 3.0”, PCI Security Standards Council LLC 2013)

PoS- (Point of Sale) eli kassajärjestelmällä tarkoitetaan tietoverkkoa, joka koostuu keskustietokoneesta ja useista siihen yhdistetyistä kassaterminaaleista. (Entrepreneur.com 2014)

AAA(Authentication, Authorization, Accounting)-protokolla on toisen osapuolen tunnistamiseen tarkoitettu verkkoprotokolla. (Urpi 2012)

Network Access Server (NAS) on ensimmäinen laite, johon käyttäjä yhdistää tulleessaan verkkoon, tarjoaa palveluita ja toimii gatewayna kaikkiin sisempiin palveluihin. (Mitton, Beadles 2000)

Remote Authentication Dial-In User Service (RADIUS) on alunperin yrityksen Livingston Entreprises Inc kehittämä AAA-protokolla. RADIUS-palvelimen ja NAS(Network access server)-palvelimen välinen kommunikaatio on UDP-pohjaista ja yhteydetöntä. RADIUS on client/server pohjainen protokolla, jossa RADIUS-client on usein NAS ja RADIUS-server UNIX- tai Windows NT-koneella ajettava daemon-prosessi. Käyttäjä ottaa yhteyden RADIUS-clientiin, joka pyytää käyttäjätunnusta ja salasanaa tai challengea Challenge Handshake Authentication Protocol(CHAP) ollessa käytössä. Käyttäjän vastatessa client lähettää tunnukset serverille, joka vastaa Accept, Reject tai Challenge (jos CHAP). (Cisco 2006)

Network Policy Server (NPS) mahdollistaa organisaationlaajuisten verkkoonpääsykäytäntöjen luonnin ja valvomisen. NPS voi myös toimia RADIUS-välityspalvelimena. (Network Policy Server 2012)

Certificate Authority on sertifikaatteja eli varmenteita myöntävä yritys.

Relaatiotietokanta on tietokanta, joka näyttää infomaatiota riveistä ja kolumneista koostuvissa tauluissa. Taulu on relaatio siinä mielessä, että se on kokoelma saman tyyppisiä objekteja. Taulun sisältämää dataa voidaan viitata yhteisten avainten tai konseptien kautta. (A Relational Database Overview 2014)

Oracle Database on Oracle Corporationin kehittämä relaatiotietokanta.

Schemalla tarkoitetaan Oracle Databasessa nimettyä tietokantaobjektien kokoelmaa, mukaanlukien loogisia rakenteita kuten tauluja ja indexejä. Schemalla on sen omistavan tietokantakäyttäjän nimi. (Oracle® Database Concepts 11g Release 2 (11.2) 2014)

Context on Oracle Databasessa kokoelma ohjelman määrittämiä attribuutteja jotka vahvistavat ja turvaavat ohjelman. SQL lause CREATE CONTEXT luo namespacen contexteille. (Oracle® Database Concepts 11g Release 2 (11.2) 2014)

Virtuaalilähiverkko (VLAN) on ryhmä verkkolaitteita joilla on yhteinen kokoelma vaatimuksia. Laitteiden fyysisellä olinpaikalla ei ole merkitystä. VLANit ovat samankaltaisia kuin lähiverkot (LAN), mutta sallivat verkkolaitteiden yhdistämisen vaikka nämä eivät ole samassa fyysisessä lähiverkossa. (VLANs, Cisco 2014)

Tom Olzakin kirjan ”Enterprise Security: A practitioner’s guide” (Olzak 2013) mukaan VLANit toimivat OSI-mallin Data-layer-tasolla (layer 2), jossa kytkimet tunnistavat verkkolaitteita näiden media access control (MAC) osoitteiden kautta. Jokaisessa verkkolaitteessa on valmistajan asettama 6-tavuinen MAC-osoite, jonka formaatti määritellään IEEE standardissa 802.2001. (Olzak 2013)

Tavanomaisessa verkossa kun tietokoneen tarvitsee kommunikoida toisen verkkolaitteen kanssa, se lähettää address resolution protocol (ARP)-lähetyksen, joka menee kytkimen läpi. 802.1D-kytkin uudelleen lähettää lähetyksen kaikkien porttien paitsi tuloportin kautta. Jos haettu laite on verkossa, se vastaanottaa ja prosessoi paketin, lähettäen vastauksen lähettäjän MAC-osoitteen kautta. Ensimmäinen ongelma tässä menetelmässä on verkon hidastuminen, koska lähetys menee kaikille laitteille. Toisena on laitteiden näkyvyys, koska mikä tahansa verkkoon yhdistetty laite voi löytää toisen laitteen lähettämällä tarvittavan määrän ARP-lähetyksiä. (Olzak 2013)

802.1Q-kytkimet pystyvät jakamaan verkon erillisiin lähetysalueisiin, VLANeihin. Tämä muuttaa edellistä esimerkkiä: nyt tietokoneen ARP-lähetys menee vain saman VLANin

laitteille, vähentäen turhaa verkkoliikennettä ja rajaten pääsyn vain tarvittaviin laitteisiin. (Olzak 2013)

Oracle Advanced Security on usein Oracle Database Enterprise Editionin kanssa käytettävä lisäominaisuus Oracle Databaseen. Se mahdollistaa kaksi toimintoa arkaluontoisen datan turvaamiseen: tietokannan kryptauksen ja näytetyn datan piilotuksen tietokannan ollessa käynnissä.

3 Segmentaatio

Verkon segmentaatiolla tarkoitetaan prosessia, jossa arkaluontoista informaatiota sisältävät verkot erotetaan muista verkoista. Segmentaation kautta voidaan keskittää tietoturvatoimenpiteet niihin verkon osiin, joissa niitä tarvitaan eniten, vähentäen tarvittavaa työtä ja aikaa. (SecureState 2014)

Verkon segmentaation tärkeys on tullut ilmi erityisesti viimeaikaisten tietomurtojen kautta, kuten Reuven Harrison kirjoittaa artikkelissaan, koska ilman oikein tehtyä segmentaatiota ulkopuolisille käyttäjille tarkoitetuilla tunnuksilla voidaan saada pääsy koko verkkoon.

Verkon segmentaatio on monissa organisaatioissa kerran asetettava asia, joka vanhenee nopeasti. Täten segmentaatiota on päivitettävä, jotta verkon turvallisuutta ei menetetä.

Lisääntyneen turvallisuuden lisäksi segmentaatio myös parantaa tehokkuutta, helpottaa ongelmien hallintaa ja vähentää verkon tukkoisuutta. Näiden parannusten hintana on prosessin vaikeus, erityisesti suurissa verkoissa jotka saattavat sisältää satoja laitteita ja suurilla organisaatiolla voi olla monimutkaisia käytäntöjä joihin kuuluu satoja sääntöjä. Organisaation täytyy siis segmentoidessaan verkkoaan ottaa huomioon jopa kymmeniä tuhansia sääntöjä turvallisuuden säilyttämiseksi. Edellä mainittujen ongelmien lisäksi useimmat organisaatiot näkevät kymmeniä muutoksia viikossa uusien toimintojen tukemiseksi sekä käyttäjien haluamat virtualisaatio- ja pilvi-palvelut tuovat omat lisänsä verkon monimutkaisuuteen. (Reuven 2014)

Standardit kuten PCI-DSS tarjoavat ohjeita datan selvään segmentaatioon, PCI-tapauksessa kortinhaltioiden data tulee eristää muusta, vähemmän arkaluontoista informaatiota sisältävästä verkosta. Esimerkkinä PoS-järjestelmät ja tietokannat tulisi täysin erottaa verkon osista, joihin ulkopuolisilla on pääsy. (Reichenberg 2014)

Tom Olzak selittää kirjassaan ”Enterprise Security: A Practitioner’s guide” (Olzak 2013) kuinka virtuaalilähiverkoilla voidaan toteuttaa verkon segmentaatio. Olzakin mukaan

tavanomaisten verkkojen ongelmana on, että vaikka nämä käyttävät palomuureja ulkopuolisten uhkia vastaan, tavanomaisilla verkoilla ei usein ole puolustuksia sisäisiä uhkia vastaan, ja täten kun hyökkääjä on päässyt verkkoon, hänellä on täysi pääsy kaikkiin järjestelmiin. VLAN-segmentaatio asettaa ylimääräisiä esteitä hyökkääjälle, vähentäen tämän saatavilla olevia järjestelmiä luomalla yhden verkon sijasta kokoelman eristettyjä verkkoja. VLAN-verkot myös mahdollistavat käyttäjien automaattisen liittämisen oikeaan verkkoon fyysisestä sijainnista huolimatta. Tämä tapahtuu trunkkauksen kautta, jossa eri kytkimissä kiinni olevien saman VLAN-verkon laitteiden ARP-lähetykset lähetetään toiseen kytkimeen trunk-portin kautta. (Olzak 2013)

VLANit voidaan konfiguroida muun muuassa portin, IP aliverkon tai protokolla mukaan, mutta roolipohjaisien käyttöoikeuksien kanssa paras vaihtoehto on dynaaminen VLAN-sijoitus, kuten Olzak kertoo kirjassaan (Olzak 2013). Dynaamisessa VLAN-sijoituksessa käyttäjä autentikoidaan tämän käyttäjäryhmän kautta RADIUS-palvelimen ja Active Directoryn kautta. Tämä menetelmä myös parantaa jaettujen VLAN-porttien turvallisuutta: esimerkkinä jos myyntihenkilö yhdistää kannettavan tietokoneensa kokoushuoneen Ethernet porttiin, kytkin vaatii laite- ja käyttäjäautentikaation. Kun RADIUS-palvelin saa käyttäjätunnukset, se käyttää Active Directorya käyttäjäryhmän määrittelyyn ja sijoittaa käyttäjän oikeaan VLAN-verkkoon, tässä esimerkissä myyntihenkilö sijoitettaisiin Myynti-VLANiin. Jos vieras yhdistää samaan porttiin, autentikaatio epäonnistuu tunnusten puuttuessa, ja laite sijoitetaan Vieras-VLANiin. (Olzak 2013)

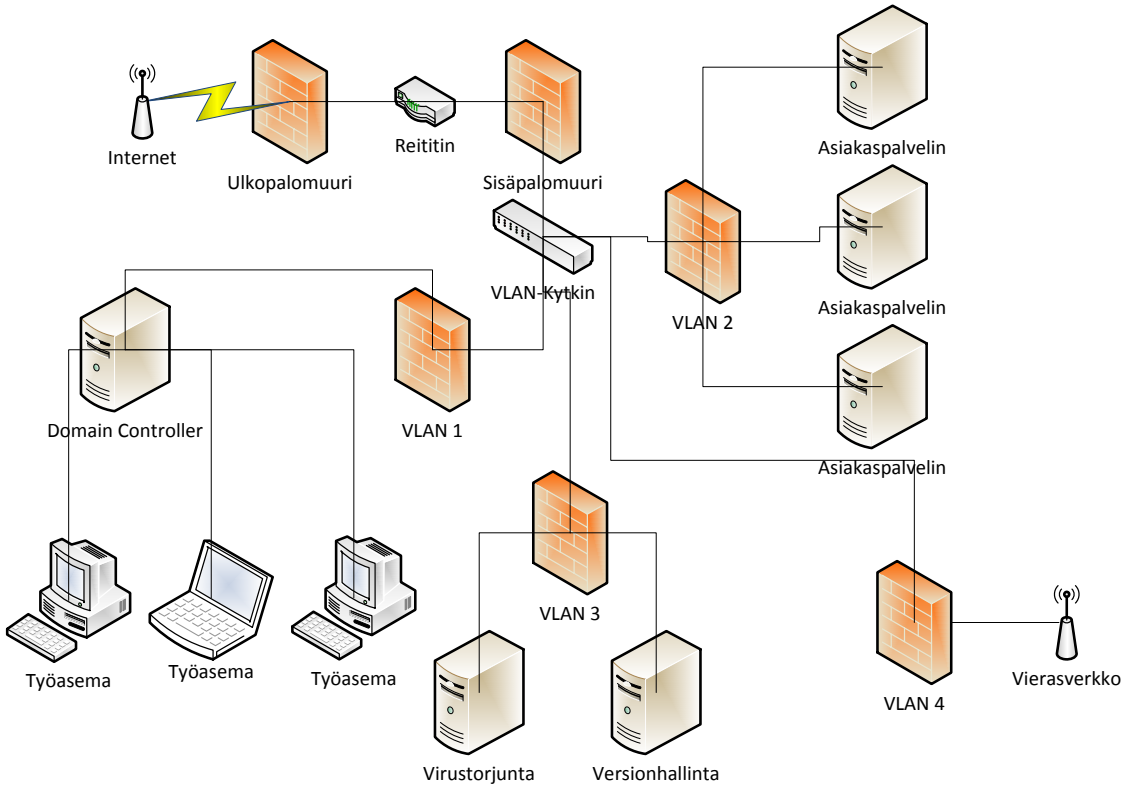
Ennen segmentaatiota yrityksen verkossa jokaisella käyttäjällä oli pääsy jokaiseen domain-liitettyyn koneeseen. Näiden lisäksi domainiin liittämättömillä palvelimilla oli erilliset admin- ja kehittäjien omat tunnukset.

Tämän sijasta ehdotan kaikkien palvelimien yhdistämistä domainiin ja AD-tunnusten käyttöä. Verkko tulisi segmentoida neljään eri virtuaalilähiverkkoon (VLAN): lähiverkko, palvelimet, sisäiset palvelut, vierasverkko. Käyttäjät tulisi jakaa viiteen eri ryhmään, jotka ovat Ylläpitäjät, joilla on pääsy kaikkiin koneisiin täysillä oikeuksilla, Kehittäjät, joilla on pääsy lähiverkkoon ja palvelimiin sekä network access että RDP-oikeuksin, Myynti**,** joilla on pääsy lähiverkkoon sekä asiakasympäristöjä sisältäviin palvelimiin network access-oikeuksin, Hallinto, joilla on pääsy vain lähiverkkoon ja viimeisenä Vieraat, joille annetaan vain internet-yhteys erillisen verkon kautta.

Koska yrityksen WLAN-verkon autentikaatio on jo RADIUS-pohjainen, mielestäni myös VLAN kannattaa asettaa edellä mainittuun dynaamiseen sijoitustilaan. Näin käyttäjän yhdistäessä tämä sijoitetaan automaattisesti oikeaan verkkoon.

4 Verkon VLAN-segmentointi

Yrityksen lähiverkko tulee jakaa neljään virtuaalilähiverkkoon (VLAN). Ensimmäisenä on LAN eli lähiverkko johon kuuluvat työasemat, Active Directory domain controller sekä käyttäjien levytila. Toisena palvelimet, johon kuuluvat asiakasympäristöja sisältävät palvelimet. Kolmantena sisäiset palvelut, johon kuuluvat yrityksen käyttämät sisäiset palvelut kuten keskitetty virustorjunta ja versionhallinta. Neljäntenä on eristetty vieraille tarkoitettu langaton lähiverkko.



Kuva 1: VLAN-segmentaatiorakenne yritysverkolle

4.1 Palvelimien rajaus käyttäjäryhmän perusteella

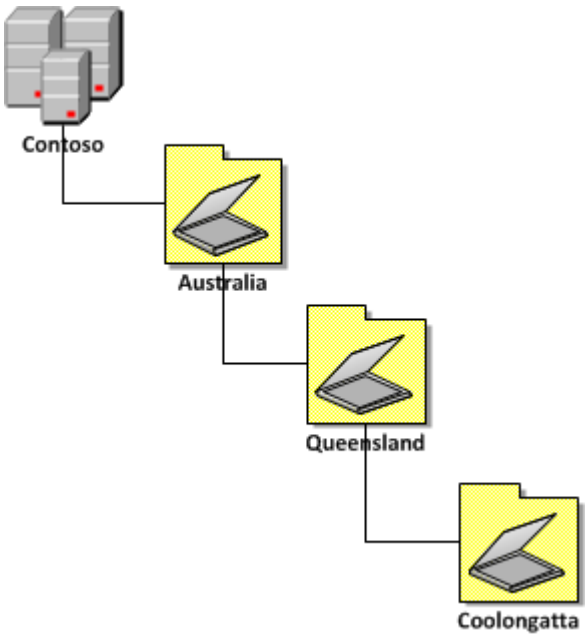
Kaikkien palvelinten ollessa yhdistettynä yrityksen Active Directory-domainiin, palvelimiin pääsy voidaan rajata käyttäjäryhmän perusteella tekemällä jokaiseen palvelimeen uusi Local Security Policy, jossa säännöt *Allow/Deny log on through Terminal Service/Remote Desktop Services* ja *Access this computer from the network* asetetaan käyttäjäryhmille.

Käyttäjäryhmistä ensimmäinen on ylläpitäjät, johon kuuluvilla käyttäjillä on täysi pääsy kaikkiin verkkoihin ja palvelimiin sekä network-access- että remote desktop-oikeuksilla. Toisena käyttäjäryhmänä on kehittäjät, johon kuuluvilla käyttäjillä on pääsy lähiverkkoon ja palvelimet-verkkoon network-access- ja remote desktop-oikeuksilla. Kolmantena

käyttäjäryhmänä on myynti, johon kuuluvilla käyttäjillä on pääsy lähiverkkoon ja asiakasympäristöjä sisältäviin palvelimiin network-access-oikeuksilla. Neljäntenä käyttäjäryhmänä on hallinto, johon kuuluvilla käyttäjillä on pääsy vain lähiverkkoon. Viimeisenä käyttäjäryhmänä on vieraat, joilla on pääsy vain vierasverkkoon, joka mahdollistaa internet-yhteyden ilman pääsyä yrityksen lähiverkkoon. Vieraat-käyttäjäryhmään kuuluu automaattisesti käytettäessä vieras-WLAN-verkkoa.

4.2 Active Directory-suunnittelu

Active Directory-rakenne on myös vaikuttava asia tietoon pääsyn rajaamisessa. Oletuksena Active Directoryyn lisättävät uudet käyttäjät lisätään ”Users”- ja ”Computers”-containereihin, jotka ovat group policyjen vaikutuksen ulkopuolella. Täten uusien käyttäjien ja tietokoneiden oletuspaikka voi olla hyödyllistä vaihtaa uusiin Active Directory-yksiköihin, joihin voidaan käyttää group policyja. Organizational unitit tulee asettaa hierarkkiseen järjestykseen tärkeimmästä vähemmän tärkeimpään kuitenkaan tekemättä liian montaa. Tämä vähentää sekavuutta suurissa verkoissa. (Burchhill 2010)



Kuva 2: Oikeaoppinen organizational unit-hierarkia (Burchhill 2010)

Organizational unitien nimeämisessä kannattaa käyttää mahdollisimman kuvaavia nimiä lyhentämättä niitä, ja samantyyppisille objekteille tarkoitetuille organizational uniteille kannattaa antaa sama nimi. Myös organizational uniteihin liitetyt group policy objectit kannattaa nimetä näiden mukaan. (Burchhill 2010)

5 WLAN

Langaton lähiverkko antaa yritykselle käyttää dataansa ilman että tietokoneiden täytyy olla kiinni kaapeleilla verkossa. Tästä on hyötyä esimerkiksi asiakaskokouksissa, mutta langaton lähiverkko voi olla turvallisuusriski, jos on konfiguroitu huonosti. Seuraava osio käsittelee kohdeyrityksen langatonta lähiverkkoa.

Ennen projektin alkamista yritys A:lla oli ongelmia langattoman lähiverkon hitauden kanssa. Tämän lisäksi vieraille ei ollut erillistä lähiverkkoa, joka huomattiin turvallisuusriskiksi. Yrityksessä päätettiin käyttää RADIUS-pohjaista PEAP-MS-CHAP v2-autentikaatiota Active Directory-tunnuksilla sisäiseen WLAN-verkkoon ja erillistä salasanapohjaista verkkoa vieraille.

PEAP-MS-CHAP v2 koostuu kahdesta pääosasta, ensin client-ohjelmisto autentikoi NPS-palvelimen. NPS-palvelin lähettää palvelinsertifikaattinsa client-tietokoneelle, jotta client voi vahvistaa palvelimen identiteetin sertifikaatille. Tämän mahdollistamiseksi client-tietokoneen on luotettava sertifikaatin myöntänyttä CA:ta. Tämän jälkeen NPS-palvelin autentikoi käyttäjän. Palvelimen autentikoinnin jälkeen client lähettää käyttäjän käyttötunnukset NPS-palvelimelle, joka vahvistaa tunnukset Active Directory Domain Services käyttäjätietokantaa vastaan. (802.1X Authenticated Wireless Deployment Guide 2014)

6 Oracle-tietokannat

Oracle Database on yksi suosituimmista tietokantaohjelmista, ja on monille yrityksille koko liiketoiminnan perusta. Kuitenkin tietokanta voi olla uhka yrityksen tietoturvalle. Kun tietokantojen määrä kasvaa, eri tietokantatunnusten hallinnointi käy hankalammaksi, ja vanhojen tunnusten poisto sekä salasanojen vaihto tulee tärkeämmäksi. Seuraava osio käsittelee Oracle Database-integraatiota Active Directoryyn.

Yrityksen Oracle-tietokannat olivat ennen toimenpiteiden alkua erillisten tunnusten kautta autentikoituina. Jokaisessa tietokannassa käytettiin erillisiä tunnuksia joka kehittäjälle, joka tekee salasanojen vaihdosta tai tunnusten poistamisesta työntekijän lähtiessä yrityksestä aikaavievää ja täten mahdollistaa turvallisuusriskien muodostumisen, jos kantaan jää vanhoja tunnuksia.

6.1 Suora Active Directory-liitto

Oracle Databasen dokumentaation mukaan Oracle Database voidaan liittää Microsoftin Active Directory-hakemistopalveluun. Tämä mahdollistaa muun muuassa tietokantapalvelinten haun

Active Directoryn kautta osoitteiden manuaalisen tnsnames.ora tiedostoon lisäämisen sijasta, tietokantojen näytön Active Directoryn kautta sekä integraation Active Directory käyttäjätunnusten kanssa, mikä poistaa edellämainitun vanhojen tunnusten muodostaman turvallisuusriskin. (Oracle® Database Platform Guide 2014, 17)

Oracle Databasen liittämiseksi Active Directoryyn vaaditaan Microsoftin ja Oraclen ohjelmistojen lisäksi oikeudet luoda Oracle schema objecteja ja Oracle Contexteja. Oracle Databasen on oltava release 8.1.6 tai myöhempi ja sekä client- että tietokantatietokoneiden on oltava Windows Server domainin jäseniä. (Oracle® Database Platform Guide 2014)

Oracle Context vaaditaan verkon kautta tehtävään palvelinten hakuun, ja se on korkeimman tason Oracle-objekti Active Directory-rakenteessa. Se sisältää Oracle Database-palvelun ja service name objekti-informaatiota.

Oracle Net Configuration Assistant (NetCA) on graafinen Oraclen verkkotoimintojen konfiguraatio- ja hallintatyökalu. Oracle Databasen liittämiseksi Active Directoryyn seuraavat toimenpiteet ovat tarvittavia:

1. Avaa Käynnistä-valikosta Oracle -> Configuration and Migration Tools -> Net Configuration Assistant.
2. Valitse Directory Usage Configuration ja klikkaa Next.
3. Valitse Directory Type Microsoft Active Directory ja klikkaa Next.
4. Valitse vaihtoehto, jossa directory konfiguroidaan Oraclen käyttöön sekä Oracle Schema ja Context luodaan ja klikkaa Next.
5. Syötä Active Directory-palvelimen hostname ja klikkaa Next.
6. Valitse vaihtoehto, jossa Oracle Schema päivitetään, ja klikkaa Next.
7. Ohjelman pitäisi ilmoittaa onnistuneesta konfiguraatiosta. Klikkaa Next ja sen jälkeen Finish.

6.2 RADIUS-AD-autentikaatio

Oracle Database voidaan myös Active Directoryyn suoraan liittämisen sijasta laittaa autentikoimaan käyttötunnukset RADIUS-palvelimen kautta. RADIUS-client on Oracle-tietokanta. Tämä menetelmä mahdollistaa, kuten Ronny Egner kirjoittaa blogissaan (Egner,R 2009), keskitetyn salasanahallinnan ja tunnuksen aktiivisuusstatuksen jo olemassa oleville käyttäjätunnuksille tietokannoissa, mutta vaatii uusien käyttäjien manuaalisen luonnin ja oikeuksien asettamisen sekä vaatii Oracle Advanced Security-option tietokantaan.

Menetelmä vaatii seuraavat toimenpiteet:

1. Syötä seuraava rivi client-tietokoneiden SQLNET.ORA-tiedostoon RADIUS-autentikaation käyttöön ottamiseksi:
    a. SQLNET.AUTHENTICATION_SERVICES=(RADIUS)
2. Syötä seuraavat rivit tietokantainstanssin SQLNET.ORA-tiedostoon:
    a. SQLNET .AUTHENTICATION_SERVICES= (radius)
    b. SQLNET.RADIUS_PORT= (1812)
    c. SQLNET.RADIUS_AUTHENTICATION_PORT = 1812
    d. SQLNET.RADIUS_SECRET = <path_to_any_directory>/radius.key
    e. SQLNET.RADIUS_AUTHENTICATION_TIMEOUT = 10
    f. #SQLNET.RADIUS_AUTHENTICATION = <RADIUS-serverin hostname tai IP-osoite, erotettuna pilkulla jos monta>
    g. SQLNET.RADIUS_AUTHENTICATION = 192.168.0.1 #Esimerkissä RADIUS-serverin IP on 192.168.0.1
    h. SQLNET.RADIUS_CHALLENGE_RESPONSE=OFF
3. "SQL.RADIUS_SECRET"-rivillä määritelty tiedosto sisältää yhteisen salasanan RADIUS-serveriin yhdistämiseen. Se määritellään RADIUS-serverin "client.conf"-tiedostossa.
4. Lisää seuraavat rivit tietokantaparametritiedostoon ja käynnistä instanssi uudelleen:
    a. REMOTE_OS_AUTHENT=FALSE
    b. OS_AUTHENT_PREFIX=""
5. Seuraavat SQL-lauseet lisäävät käyttäjän tietokantaan ulkoisesti autentikoituna:
    a. create user <username> identified externally;
    b. grant create session to <username>;
6. Olemassa olevan käyttäjän autentikaation muutos:
    a. alter user <username> identified externally;
7. Tietokannan ja Active Directoryn käyttäjänimien on sovittava yhteen. Jos näin ei ole, RADIUS voidaan asettaa muuttamaan käyttäjänimet sopimaan.
8. RADIUS-konfiguraatio:
    a. radiusd.conf
        i. # module configuration section
        ii. ldap {
        iii. server = "ad01.yritys.fi"
        iv. identity = "cn=radiusadmin,cn=users,dc=yritys,dc=fi"
        v. password = test
        vi. basedn = "ou=users,DC=yritys,DC=fi"
        vii. dictionary_mapping = ${raddbdir}/ldap.attrmap
        viii. filter = (&(&(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})(&(objectCategory=person)(objectClass=user)(
        ix. !(userAccountControl:1.2.840.113556.1.4.803:=2)))))
        x. password_attribute = "userPassword"

xi. timeout = 10
xii. timelimit = 10
xiii. net_timeout = 1
xiv. ldap_connections_number = 5
xv. compare_check_items = no
xvi. }

b. Muuttujat:
   i. Server: Active Directory-palvelin
   ii. Identity: käyttäjätunnus Active Directoryyn yhdistämiseen
   iii. Password: salasana Identity-kohdassa määritellylle käyttäjätunnukselle
   iv. Basedn: käyttäjän salasana etsitään tästä Active Directoryssa
   v. Dictionary_mapping: tiedosto tulee freeRADIUS:n mukana
   vi. Filter: Ronny Egnerin filter, tarkistaa käyttäjätunnuksen salasanan ja aktiivisuuden.
   vii. Password_attribute: salasanan sisältävä LDAP-kenttä
   viii. compare_check_items: Määrittää, vertaako moduuli saapuvan pyynnön check itemejä LDAP:in sisältämiin

c. Ota käyttöön LDAP-autentikaatio lisäämällä tai epäkommentoimalla radiusd.conf-tiedoston authentication-osioissa:
   i. #authentication section
   ii. Auth-Type LDAP {
   iii. ldap
   iv. }

d. client.conf
   i. Tämä tiedosto sisältää asetuksia RADIUS-palvelimeen yhdistäville clienteille. Esimerkissä käytetty tietokantapalvelimen IP-osoite on 192.168.0.10
      1. client 192.168.0.10 {
      2. secret = testing123
      3. shortname = dbserver #for identification only... doesnt matter at all
      4. }
   ii. ”secret”-osion ”testing123” on tietokantaserverin ja RADIUSin yhteinen salasana, joten tämä on lisättävä ”SQLNET.RADIUS_SECRET”-osiossa määriteltyyn tiedostoon. (Egner,R 2009)

7 Käyttäjäoikeudet

Kaikki edellämainitut segmentaatio- ja tietoturvatoimet vaativat tarkasti määritellyt ja toimivat käyttäjäoikeudet. Active Directory Domain Services (AD DS) oikein konfiguroituna toteuttaa tämän tarpeen käyttäjäryhmillä ja Group Policylla.

Active Directory Domain Services-käyttäjäryhmät ovat directory objekteja, jotka sijaitsevat domainin organizational unit-container objekteissa, ja niitä voidaan käyttää hallinnoinnin yksinkertaistamiseen antamalla jaetun resurssin käyttöoikeudet yksittäisten käyttäjien sijasta ryhmälle. Group Policy mahdollistaa samojen sääntöjen käytön kaikissa domainiin liitetyissä tietokoneissa. Tämä antaa kaikille ryhmän jäsenille samat oikeudet resurssiin.

8 Yhteenveto ja johtopäätökset

Tutkielman alkuongelmana oli yrityksen tietoverkon tietoturvan parantaminen verkon segmentaatiota käyttäen. Projektin edetessä huomattiin prosessiin liittyvän VLAN-segmentaation lisäksi Active Directory-käyttäjäryhmien luonti sekä näiden yhdistäminen VLAN-verkkoihin, WLAN-autentikaatioon sekä Oracle Database-autentikaatioon. Nämä osat tekevät segmentaatio prosessista monimutkaisemman, mutta myös turvallisemman.

Projektin tavoitteena oli verkon tietoturvan vahvistuminen, ja mielestäni tämä tutkielma antaa valmiudet siihen. VLAN-segmentaatio rajoittaa tunkeutujan pääsyn yritysverkossa tämän tunkeutumaan segmenttiin ja Active Directory-käyttäjäryhmät rajoittavat pääsyn tunkeutujan käytössä olevaan käyttäjäryhmään.

Ensimmäinen luku, ”johdanto” käsittelee tutkielman aihetta ja sen tekotarkoitusta, tutkimusongelmaa ja – kysymyksiä, sen viitekehystä, raportin rakennetta sekä aikataulua. Toinen luku, ”tietoperusta” käsittelee raportin peruskäsitteitä. Kolmas luku, ”segmentaatio” käsittelee segmentaatiota teoreettisesti. Neljäs luku, ”VLAN-segmentaatio” käsittelee segmentaatiota käytännössä. Viides luku, ”WLAN” käsittelee langattomia lähiverkkoja ja niiden osaa verkon segmentaatiossa. Kuudes luku, ”Oracle-tietokannat” käsittelee Oracle Database-integraatiota Active Directoryyn ja tämän hyötyä segmentaatiossa. Seitsemännessä luvussa käsitellään käyttäjäoikuksia

Jatkopiteisiin VLAN-segmentaatiossa kuuluu tärkeimpänä segmentaation säännöllinen uudelleen analysointi. Ilman säännöllistä uudelleen analysointia segmentaation hyödyllisyys vähenee huomattavasti, kun tunkeutujilla on aikaa tutkia verkon rakennetta.

Tutkielman tarkoituksena ja tavoitteena oli verkon segmentaation hyötyjen sekä segmentaation käytännön toteutusta sekä yrityksen tietoturvan parantuminen. Näkemykseni on, että se onnistui molemmissa tavoitteissa. Segmentaation hyödyt tulevat esiin, ja raportti

antaa myös pohjan yrityksen verkon segmentaatioon käytännössä. Täten johtopäätöksenä on, että tutkielma onnistui tavoitteessaan.

9 Lähteet

"So What Is Active Directory?", Microsoft, käyty 23.12.2014, http://msdn.microsoft.com/en-us/library/aa746492%28v=vs.85%29.aspx

"Active Directory Domain Services", Microsoft, käyty 23.12.2014, http://msdn.microsoft.com/en-us/library/aa362244(v=vs.85).aspx

"Organizational units", Microsoft, 21.1.2005, http://technet.microsoft.com/en-us/library/cc758565%28v=ws.10%29.aspx

"Payment Card Industry (PCI) Data Security Standard 3.0", PCI Security Standards Council LLC, Marraskuu 2013

"Active Directory Structure Guidelines – Part 1", Burchill, Alan, 23.7.2010, http://www.grouppolicy.biz/2010/07/best-practice-active-directory-structure-guidelines-part-1/2/

"Network Segmentation Key To Good Network Hygiene", Harrison, Reuven, 6.6.2014, http://www.networkcomputing.com/networking/network-segmentation-key-to-good-network-hygiene/a/d-id/1269687

"Network Segmentation", SecureState, käyty 23.12.2014, http://www.securestate.com/Services/Risk%20Management/Pages/Network-Segmentation.aspx

"Point of Sale (POS) System", Entrepreneur.com, käyty 23.12.2014, http://www.entrepreneur.com/encyclopedia/point-of-sale-pos-system

"Improving Security via Proper Network Segmentation", Reichenberg, Nimmy, 20.3.2014, http://www.securityweek.com/improving-security-proper-network-segmentation

"How Does RADIUS Work?", Cisco, 19.1.2006, http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/12433-32.html

"FreeRADIUS for small and medium-sized companies", Urpi, Joonas, 2012, http://www.theseus.fi/handle/10024/47101

"Network Policy Server", Microsoft, 29.3.2012, http://msdn.microsoft.com/en-us/library/cc732912.aspx

"802.1X Authenticated Wireless Deployment Guide", Microsoft, Käyty 29.12.2014, http://technet.microsoft.com/en-us/library/dd283093%28v=ws.10%29.aspx

"Oracle® Database Platform Guide", Oracle, käyty 29.12.2014

"Network Access Server Requirements Next Generation (NASREQNG)",Mitton.D, Beadles.M, kesäkuu 2000, http://tools.ietf.org/html/rfc2881

"A Relational Database Overview", Oracle, käyty 29.12.2014, http://docs.oracle.com/javase/tutorial/jdbc/overview/database.html

"Oracle® Database Concepts 11g Release 2 (11.2)", Oracle, käyty 29.12.2014, https://docs.oracle.com/cd/E18283_01/server.112/e16508/glossary.htm#CHDIJCIE

"Enterprise Security: A practitioner's guide." Olzak,T., 2013, http://resources.infosecinstitute.com/vlan-network-chapter-5/

"VLANs", Cisco, käyty 30.12.2014, http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vlans.html

"Authentificate Oracle user passwords against Active Directory using Radius", Egner,R., 16.11.2009, http://blog.ronnyegner-consulting.de/2009/11/16/authentificate-oracle-user-passwords-against-active-directory-using-radius/

Kuvat